

SonicWall SonicOS 6.5.4.15

Release Notes

September 2024

These release notes provide information about the SonicWall SonicOS 6.5.4.15 release.

Topics:

- [About SonicOS 6.5.4.15](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Additional References](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicOS 6.5.4.15

SonicWall SonicOS 6.5.4.15 resolved key issues, which were found since the previous release. For more information, refer to the [Resolved Issues](#) section. This release supports all the features and contains all the resolved issues found in previous SonicOS 6.5 releases. The previous release notes are available on MySonicWall at: <https://mysonicwall.com>.

IMPORTANT: SonicWall strongly advises that customers using Gen6 firewalls with SSL VPN users who have locally managed accounts immediately update their passwords to enhance security and prevent unauthorized access. Users can change their passwords if the **User must change password** option is enabled on their account. Administrators must manually enable the **User must change password** option for each local account to ensure this critical security measure is enforced.

To set the **User must change password** option, navigate to **MANAGE | System Setup > Users > Local Users & Groups**. For details refer to “Configuring Local Users Settings,” a section in the [SonicOS 6.5 System Setup Administration Guide](#).

Additionally, SonicWall recommends enabling multi-factor authentication (MFA), either TOTP or Email-based OTP, for all SSL VPN users. Refer to [How Do I Configure 2FA for SSL VPN with TOTP?](#) for more information.

Supported Platforms

SonicOS 6.5.4.15 is supported on the following SonicWall appliances:

- NSa 9650
- NSa 9450
- NSa 9250
- NSa 6650
- NSa 5650
- NSa 4650
- NSa 3650
- NSa 2650
- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- TZ600 / TZ600P
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ350 / TZ350 Wireless
- TZ300 / TZ300P / TZ300 Wireless
- SOHO 250 / SOHO 250 Wireless
- SOHO Wireless

Resolved Issues

This section provides a list of resolved issues in this release.

Resolved Issue	Issue ID
SonicOS improper access control vulnerability (SNWLD-2024-0015).	Gen6-4345
NetExtender client version updated to 10.2.341.	GEN6-4328
App Rules over DPI-SSL are not working when TLS hybridized kyber support is enabled on Chrome which is now enabled by default.	GEN6-4286
Critical SSL-VPN fixes accumulated from prior hotfixes.	GEN6-4282
CFS blocking over DPI-SSL is not working when TLS hybridized kyber support is enabled on Chrome, which is now enabled by default.	GEN6-4272
Login fails when user with accent characters in name are using LDAP authentication.	GEN6-4268
SSL VPN zip file, which includes all SSL VPN client files, has not been updated with the latest versions of the clients.	GEN6-4244
Instead please download the latest version of the VPN clients from https://www.sonicwall.com/products/remote-access/vpn-clients/ .	

Known Issues

There are no known issues for this release.

Additional References

GEN6-4330, GEN6-4273, GEN6-4259, GEN6-4258, GEN6-4209, GEN6-4162, GEN6-4130, GEN6-3958, GEN6-3841, GEN6-3808, GEN6-3799, GEN6-3792, GEN6-3775, GEN6-3752, GEN6-3623, GEN6-3514, GEN6-3501, GEN6-3423, GEN6-3395, GEN6-3364, GEN6-3358, GEN6-3353, GEN6-3327, GEN6-3281, GEN6-3274, GEN6-3272, GEN6-3269, GEN6-3268, GEN6-3248, GEN6-3247, GEN6-3231, GEN6-3225, GEN6-3092, GEN6-2836, GEN6-2654, GEN6-2508, GEN6-2241, GEN6-2137

System Compatibility

This section provides additional information about hardware and software compatibility with this release.

Wireless 3G/4G Broadband Devices

SonicOS 6.5.4 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:

<https://www.sonicwall.com/support/knowledge-base/what-wireless-cards-and-broadband-devices-are-supported-on-sonicwall-firewalls-and-access-points/170505473051240/>

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 9.3.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, Edge or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- Edge 81.0 and higher
- Safari 10.0 and higher running on non-Windows machines

NOTE: On Windows machines, Safari is not supported for SonicOS management.

NOTE: Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.5 Upgrade Guide* available on the Support portal at <https://www.sonicwall.com/support/technical-documentation>.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View [knowledge base articles](#) and [technical documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [video tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall professional services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

Copyright © 2024 SonicWall Inc. All rights reserved.




This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.